

UNITED STATES PATENT APPLICATION

FOR

SECURE USER AUTHENTICATION TO COMPUTING RESOURCE VIA SMART
CARD

Inventors:

Brian Rasmussen
Matthew Harmsen

Prepared by:
WAGNER, MURABITO & HAO, LLP
Two North Market Street
Third Floor
San Jose, California 95113
(408) 938-9060

106290" 0556860

1
2
3
4
5 **SECURE USER AUTHENTICATION TO COMPUTING**
6 **RESOURCE VIA SMART CARD**
7
8
9

10 **FIELD OF THE INVENTION**

11 This invention relates generally to the field of computer security. More
12 particularly, this invention relates to use of smart cards to provide access to
13 computing resources.
14

15 **BACKGROUND OF THE INVENTION**

16 Smart cards are currently used in some environments to provide secure
17 access to high security computing resources. Typically, a user receives a smart
18 card and PIN (Personal Identification Number) from a network administrator. The
19 smart card is then activated by the network administrator after a sequence of
20 communications between the network administrator and the user. The current
21 procedures can be time consuming for both the user and the network administrator.

22 Once the smart card is activated, the user obtains access to computing
23 resources by inserting the smart card into a smart card reader at a computer
24 workstation or the like and enters a PIN code on a touchpad or from a keyboard.
25 Such use of smart cards provides a relatively high level of security against
26 unauthorized use of a computing resource, but is not without drawbacks.

27 As previously mentioned, the process of activating smart cards is currently
28 a time consuming manual process. Moreover, since the smart card often resides
29 in the smart card reader during the course of a user's session, the user is prone to

1 forgetting the smart card - leaving it in the reader and thus compromising security.
2 Although smart cards are currently used primarily in very high security
3 environments, the cost of these smart cards is dropping rapidly, making them
4 suitable for use in environments with less stringent security requirements, and often
5 with less sophisticated users.
6

7 SUMMARY OF THE INVENTION

8 The present invention relates generally to computer security. Objects,
9 advantages and features of the invention will become apparent to those skilled in
10 the art upon consideration of the following detailed description of the invention.

11 In one embodiment of the present invention a simplified user authentication
12 to a computer resource is provided utilizing a smart card. When a new user is
13 issued a smart card, he or she is also issued a user name (ID) and password to be
14 used during a first use to activate the smart card. The user then connects the
15 smart card and enters the user ID and password. The user is authenticated using
16 the user ID and password and identifying information from the smart card. The
17 network administration server then requests a public key from the workstation. The
18 workstation instructs the smart card to generate public and private key. The public
19 key is transmitted to the server. A digital certificate is created the smart card is
20 activated. Once the smart card is activated a simplified login procedure can be
21 used wherein connecting the smart card to a workstation initiates a login process
22 not requiring use of a PIN number or other user input.

23 In one embodiment consistent with the present invention, a method of using
24 a smart card, includes issuing a smart card to a user; issuing manual
25 authentication information to the user; authenticating the user and the smart card
26 using the manual authentication information; obtaining a public key from the smart
27 card; and issuing a digital certificate using the public key to the smart card to
28 activate the smart card.

29 Another method, consistent with an embodiment of the present invention,
30 of using a smart card includes receiving a smart card; receiving manual

1 authentication information; authenticating the smart card using the manual
2 authentication information; generating a public key using the smart card; sending
3 the public key to an administration server; and receiving a digital certificate
4 generated using the public key to activate the smart card.

5 Another method, consistent with an embodiment of the present invention,
6 of using a smart card, includes connecting the smart card to a workstation; sending
7 a login request to a server; authenticating a digital certificate for the smart card; and
8 if authenticated, permitting a login to a computer resource.

9 The above summaries are intended to illustrate exemplary embodiments of
10 the invention, which will be best understood in conjunction with the detailed
11 description to follow, and are not intended to limit the scope of the appended
12 claims.

13 BRIEF DESCRIPTION OF THE DRAWINGS

14 The features of the invention believed to be novel are set forth with
15 particularity in the appended claims. The invention itself however, both as to
16 organization and method of operation, together with objects and advantages
17 thereof, may be best understood by reference to the following detailed description
18 of the invention, which describes certain exemplary embodiments of the invention,
19 taken in conjunction with the accompanying drawings in which:

20 **FIGURE 1** is a block diagram of a system suitable for use of an embodiment
21 consistent with the present invention.

22 **FIGURE 2** is a flow chart of a smart card activation process consistent with
23 an embodiment of the present invention.

24 **FIGURE 3** is a block diagram of another system suitable for use of an
25 embodiment consistent with the present invention.

26 **FIGURE 4** is a flow chart depicting modifications of the smart card activation
27 process of **FIGURE 2** consistent with another embodiment of the present invention.
28

1 **FIGURE 5** illustrates an exemplary administrative screen shot for
2 establishing a level of smart card login security.

3 **FIGURE 6** is a flow chart illustrating a process consistent with an
4 embodiment of the present invention for use of a smart card for simplified access
5 to a computing resource.

6 7 **DETAILED DESCRIPTION OF THE INVENTION**

8 In the following detailed description of the present invention, numerous
9 specific details are set forth in order to provide a thorough understanding of the
10 present invention. However, it will be recognized by one skilled in the art that the
11 present invention may be practiced without these specific details or with
12 equivalents thereof. In other instances, well known methods, procedures,
13 components, and circuits have not been described in detail as not to unnecessarily
14 obscure aspects of the present invention.

15 16 **NOTATION AND NOMENCLATURE**

17 Some portions of the detailed descriptions which follow are presented in
18 terms of procedures, steps, logic blocks, processing, and other symbolic
19 representations of operations on data bits that can be performed on computer
20 memory. These descriptions and representations are the means used by those
21 skilled in the data processing arts to most effectively convey the substance of their
22 work to others skilled in the art. A procedure, computer executed step, logic block,
23 process, etc., is here, and generally, conceived to be a self-consistent sequence
24 of steps or instructions leading to a desired result. The steps are those requiring
25 physical manipulations of physical quantities.

26 Usually, though not necessarily, these quantities take the form of electrical
27 or magnetic signals capable of being stored, transferred, combined, compared, and
28 otherwise manipulated in a computer system. It has proven convenient at times,
29 principally for reasons of common usage, to refer to these signals as bits, values,

elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as "processing" or "computing" or "authenticating" or "initiating" or "determining" or "obtaining" or "sending" or "verifying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

SECURE USER AUTHENTICATION TO COMPUTING RESOURCE VIA SMART CARD IN ACCORDANCE WITH THE INVENTION

While this invention is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail specific embodiments, with the understanding that the present disclosure is to be considered as an example of the principles of the invention and not intended to limit the invention to the specific embodiments shown and described. In the description below, like reference numerals are used to describe the same, similar or corresponding parts in the several views of the drawings.

Turning now to **FIGURE 1**, an exemplary network 100 is illustrated. A smart card 110 can be inserted into an appropriate connector in a smart card reader 114. Smart card reader 114 is connected to, or forms apart of, a workstation 120 connected to a computer network 126. Access to the network resources and issuance of smart cards, passwords, login identification, etc. is administered using an administration server 130 which is coupled to network information services or

1 directory services (NIS/DS) database 134. In network 100, administration server
2 130 also provides the function of administration of digital certificates. Smart card
3 110 is utilized by a user to obtain access to any of the computing resources
4 available in network 126 including various file servers and the like. Depending
5 upon the level of security required, it may be desirable to permit a user to login
6 using smart card 110 as the only authentication mechanism. That is, while
7 conventional security systems require a smart card 110 in combination with
8 personal identification number PIN, in less secure situations it may be useful to
9 permit connection of the smart card 110 to initiate a user login. Moreover, it may
10 also be desirable to permit a user to activate a smart card 110 without intensive
11 involvement of network administration personnel.

12 **FIGURE 2** illustrates a simplified smart card activation process 200 starting
13 at 204. When a new user is to be allowed access to computing resources, the new
14 user is issued a smart card 110 at 208 and a user name (user ID) and password
15 at 212. If, at 218, the smart card 110 is not being used for the first time, control
16 passes to 230 where normal operation is carried out with the user logging in by
17 connecting the smart card 110 at 230. Upon the first use of the smart card 110 at
18 218, the user connects the smart card 110 at 234 and enters his or her user ID and
19 password. The network administration server receives the user ID and password
20 as well as identifying information from the smart card 110 at 238.

21 If at 242 the user is not properly authenticated, then the login is rejected at
22 246. If the smart card 110 is properly authenticated at 242, control passes to 250
23 where the server requests a public key from the smart card 110. The workstation
24 120 requests a pair of keys (a public key and a private key) from the smart card 110
25 and sends the public key to the administration server. At 254, a certificate
26 authority, in this case coexisting with the administration server 130, creates a digital
27 certificate using the public key and information from the NIS/DS database and
28 sends the certificate to the workstation 120 at 260. At 266 of the smart card 110
29 is thus activated upon receipt of the digital certificate. The digital certificate may
30 be stored at the smart card 110 or workstation 120 or simply retained at the

1 certificate authority and towards the administration server. The activation process
2 ends at 270.

3 In the example just described, the administration server 130 also has the role
4 of certificate authority (CA). However, the certificate authority may be a separate
5 entity as illustrated in exemplary network 300 of **FIGURE 3**. In this example, the
6 administration server 132 provides network administration services while a
7 separate certificate authority 140 is also coupled to the network to handle issuance
8 of digital certificates. Certificate authority 140 may reside locally or be connected
9 to the network 126 via the Internet or other wide area or local area network. The
10 simplified authentication process described in connection with exemplary network
11 100 and process 200 can be carried out in much the same manner with slight
12 modifications as illustrated by process 400 of **FIGURE 4**.

13 Process 400 begins after 250 of process 200 and substitutes for 254 and
14 260. When the server requests a public key at 250 of process 200, control passes
15 to 454 of 400 where the workstation 120 requests the smart card 110 to generate
16 a key pair (public and private) and sends the public key to the administration server.
17 The administration server requests the certificate from the certificate authority at
18 458 and the certificate authority creates a digital certificate using the public key and
19 information obtained from the administration server at 460. Control then passes
20 to 266 and 270 as in process 200.

21 Thus, the activation of the smart card 110 is simplified by requiring minimal
22 network administration action with the smart card 110 being essentially self
23 activating upon the user initiating a first login using user ID and password. After
24 this initial login, the normal login procedure can be determined by the setup of the
25 user login parameters within the network. **FIGURE 5** illustrates as screen shot 500
26 of a smart card login configuration window showing several exemplary possible
27 login scenarios that can be provided (in whole or in part) once the user's smart card
28 110 is authenticated. In one scenario, suitable for lower security applications, a
29 user can login to the network using only the smart card 110 without need for a PIN,

1 password or user ID. Other scenarios, increasing in security level from top to
2 bottom, can also be provided.

3 In one login scenario, a smart card 110 can be used to automate the login
4 process for users not requiring the highest levels of security. In this scenario, the
5 user is authenticated using the smart card 110 in accordance with the process
6 described above, providing the authentication for the card holder without need for
7 PIN, password or user ID. Of course, this results in a lower level of security and
8 makes a system vulnerable to access using borrowed, lost or stolen smart cards.
9 However, in some networks for some users, this may provide an acceptable
10 security risk in exchange for the simplification in login.

11 Process 230 of **FIGURE 6** describes use of a smart card 110 as an aide to
12 simplified login and to provide authentication starting at 604. At 610, the process
13 determines if the smart card 110 is connected, and if not, awaits connection of a
14 smart card 110. Once a smart card 110 is connected to the workstation 120 at
15 610, the smart card 110, in conjunction with the workstation 120, initiates a login
16 at 616. This may be accomplished, for example, by sending a message out over
17 the network alerting network servers that a smart card 110 is connected. The smart
18 card 110 is then authenticated at 620. This may be accomplished, for example, by
19 challenging the smart card 110 to carry out an encryption operation using its
20 private key. If the encrypted information can be correctly decrypted at the server
21 using the public key, then it is presumed that the smart card 110 is properly
22 authenticated. The authentication process of 620 also utilizes the digital certificate
23 and verifies that the certificate has not been revoked at 640 as a further portion of
24 the authentication process. If the certificate is not good (for example if the
25 certificate is indicated as having been revoked by its presence on a certificate
26 revocation list) the login is rejected at 654. If the certificate is good at 648, login is
27 authorized at 660 and process ends at 668.

28 Using process 230 of **FIGURE 6**, the user can easily initiate a login by
29 simply inserting the smart card 110 into smart card reader 114 and awaiting an on

1 screen indication of a completed login. Since loss of a card is perhaps the most
2 serious threat to security in such a system, it is desirable that in one embodiment,
3 the card be removed after the authentication is complete. Thus, the user inserts
4 the card until login is complete and then removes the card to carry out a session
5 on the computer resource. When the session is complete, the user logs out to
6 prohibit unauthorized use.

7 Thus, the present invention provides for a simplified mechanism for
8 activating a smart card and for logging into a computer network. Many variations
9 will occur to those skilled in the art.

10 Those skilled in the art will recognize that the present invention has been
11 described in terms of exemplary embodiments based upon use of a programmed
12 processor. However, the invention should not be so limited, since the present
13 invention could be implemented using hardware component equivalents such as
14 special purpose hardware and/or dedicated processors which are equivalents to
15 the invention as described and claimed. Similarly, general purpose computers,
16 microprocessor based computers, micro-controllers, optical computers, analog
17 computers, dedicated processors and/or dedicated hard wired logic may be used
18 to construct alternative equivalent embodiments of the present invention.

19 Those skilled in the art will appreciate that the program steps used to
20 implement the embodiments described above can be implemented using disc
21 storage as well as other forms of storage including Read Only Memory (ROM)
22 devices, Random Access Memory (RAM) devices; optical storage elements,
23 magnetic storage elements, magneto-optical storage elements, flash memory, core
24 memory and/or other equivalent storage technologies without departing from the
25 present invention. Such alternative storage devices should be considered
26 equivalents.

27 The present invention is preferably implemented using a programmed
28 processor executing programming instructions that are broadly described above in
29 flow chart form, and that can be stored in any suitable electronic storage medium
30 or that can be transmitted over any electronic communication medium. However,

1 those skilled in the art will appreciate that the processes described above can be
2 implemented in any number of variations and in many suitable programming
3 languages without departing from the present invention. For example, the order of
4 certain operations carried out can often be varied, and additional operations can be
5 added without departing from the invention. Error trapping can be added and/or
6 enhanced and variations can be made in user interface and information
7 presentation without departing from the present invention. Such variations are
8 contemplated and considered equivalent.

9 While the invention has been described in conjunction with specific
10 embodiments, it is evident that many alternatives, modifications, permutations and
11 variations will become apparent to those skilled in the art in light of the foregoing
12 description. Accordingly, it is intended that the present invention embrace all such
13 alternatives, modifications and variations as fall within the scope of the appended
14 claims.

15 What is claimed is:
16